Commission Delegated Regulation (EU) 2017/392 of 11 November 2016 supplementing Regulation (EU) No 909/2014 of the European Parliament and of the Council with regard to regulatory technical standards on authorisation, supervisory and operational requirements for central securities depositories (Text with EEA relevance)

CHAPTER X

OPERATIONAL RISKS

(Article 45(1) to (6) of Regulation (EU) No 909/2014)

SECTION 4

Business continuity

Article 76

Strategy and policy

1 A CSD shall have a business continuity policy and associated disaster recovery plan that is:

a approved by the management body;

b subject to audit reviews that shall be reported to the management body.

2 A CSD shall ensure that the business continuity policy:

a identifies all its critical operations and IT systems and provides for a minimum service level to be maintained for those operations;

b includes the CSD's strategy and objectives to ensure the continuity of operations and systems referred to in point (a);

c takes into account any links and interdependencies to at least:

(i) users;

(ii) critical utilities and critical service providers;

(iii) other CSDs;

(iv) other market infrastructures;

d defines and documents the arrangements to be applied in the event of a business continuity emergency or major disruption of the CSD's operations in order to ensure a minimum service level of critical functions of the CSD;

e identifies the maximum acceptable period of time which critical functions and IT systems may be out of use.

3 A CSD shall take all reasonable steps to ensure that settlement is completed by the end of the business day even in case of a disruption, and that all the users' positions at the time of the disruption are identified with certainty in a timely manner.

Article 77

Business impact analysis

1 A CSD shall conduct a business impact analysis to:

a prepare a list with all the processes and activities that contribute to the delivery of the services it provides;

b identify and create an inventory of all the components of its IT system that support the processes and activities identified in point (a) as well as their respective interdependencies;

c identify and document qualitative and quantitative impacts of a disaster recovery scenario to each process and activity referred to in point (a) and how the impacts change over time in case of disruption;

d define and document the minimum service levels considered acceptable and adequate from the perspective of the users of the CSD;

e identify and document the minimum resource requirements concerning personnel and skills, work space and IT to perform each critical function at the minimum acceptable level.

2 A CSD shall conduct a risk analysis to identify how various scenarios affect the continuity of its critical operations.

3 A CSD shall ensure that its business impact analysis and risk analysis fulfil all of the following requirements:

a they are kept up to date;

b they are reviewed following a material incident or significant operational changes and, at least, annually;

c they take into account all relevant developments, including market and IT developments.

Article 78

Disaster recovery

1 A CSD shall have in place arrangements to ensure the continuity of its critical operations in disaster scenarios, including natural disasters, pandemic situations, physical attacks, intrusions, terrorist attacks, and cyber-attacks. Those arrangements shall ensure:

a the availability of adequate human resources;

b the availability of sufficient financial resources;

c the failover, recovery and resuming of operations in a secondary processing site.

2 The CSD's disaster recovery plan shall identify and include a recovery-time objective for critical operations and determine for each critical operation the most suitable recovery strategies. The recovery-time objective for each critical operation shall not be longer than two hours. The CSD shall ensure that back-up systems commence processing without undue delay unless this would jeopardise the integrity of the securities issues or the confidentiality of the data maintained by the CSD. A CSD shall ensure that two hours from a disruption, it is capable of resuming its critical operations. In determining the recovery times for each operation, the CSD shall take into account the potential overall impact on the market efficiency. Those arrangements shall at least ensure that, in extreme scenarios, agreed service levels are met.

3 A CSD shall maintain at least a secondary processing site with sufficient resources, capabilities, functionalities and staffing arrangements, which are adequate to the CSD's operational needs and risks that the CSD faces in order to ensure continuity of critical operations, at least in case the main location of business is not available.

The secondary processing site shall:

a provide the level of services necessary to ensure that the CSD performs its critical operations within the recovery time objective;

b be located at a geographical distance from the primary processing site that allows the secondary processing site to have a distinct risk profile and prevents it from being affected by the event affecting the primary processing site;

c is immediately accessible by the CSD's staff in order to ensure continuity of its critical operations where the primary processing site is not available.

4 A CSD shall develop and maintain detailed procedures and plans concerning:

a the identification, logging and reporting of all disruptive events for the operations of the CSD;

b response measures to operational incidents and emergency situations;

c the assessment of damages, and appropriate plans for activating the response measures referred to in point (b);

d crisis management and communications, including appropriate contact points, to ensure that reliable and up to date information is transmitted to relevant stakeholders and the competent authority;

e the activation and transition to alternative operational and business sites;

f IT recovery, including activation of the secondary IT processing site and failover.

Article 79

Testing and monitoring

A CSD shall monitor its business continuity policy and disaster recovery plan and test them at least annually. The CSD shall also test its business continuity policy and disaster recovery plan after substantive changes to the systems or related operations in order to ensure that the systems and operations achieve the CSD objectives. The CSD shall plan and document these tests, which shall include:

(a) scenarios of large scale disasters;

(b) switchovers between the primary processing site and secondary processing site;

(c) the participation of, as appropriate:

(i) users of the CSD;

(ii) critical utilities and critical service providers;

(iii) other CSDs;

(iv) other market infrastructures;

(v) any other institution with which interdependencies have been identified in the business continuity policy.

Article 80

Maintenance

1 A CSD shall regularly review and update its business continuity policy and disaster recovery plan. The review shall include all critical operations of a CSD and provide for the most suitable recovery strategy for those operations.

2 When updating the business continuity policy and disaster recovery plan, a CSD shall take into consideration the outcome of the tests and recommendations from the audit reviews and from the competent authority.

3 A CSD shall review its business continuity policy and disaster recovery plan after every significant disruption of its operations. That review shall identify the causes of the disruption and any required improvement to the CSD's operations, the business continuity policy and disaster recovery plan.

Changes to legislation:
Commission Delegated Regulation (EU) 2017/392, SECTION 4 is up to date with all changes known to be in force on or before 23 July 2024. There are changes that may be brought into force at a future date. Changes that have been made appear in the content and are referenced with annotations.
EUR 2017 No. 392 may be subject to amendment by EU Exit Instruments made by the Bank of England under powers set out in The Financial Regulators' Powers (Technical Standards etc.) (Amendment etc.) (EU Exit) Regulations 2018 (S.I. 2018/1115), regs. 2, 3, Sch. Pt. 3. These amendments are not currently available on legislation.gov.uk. Details of relevant amending instruments can be found on their website/s.
View outstanding changes

Changes and effects yet to be applied to :

– Regulation revoked by 2023 c. 29 Sch. 1 Pt. 13